CLAIMS

1. An intelligent identification card comprising:

an on-board memory for storing reference data,

an on-board sensor for capturing live biometric data,

an on-board microprocessor for comparing the captured biometric data with corresponding stored reference data within a predetermined threshold and for generating a verification message only if there is a match within a predetermined threshold, and

means for communicating the verification message to an external network.

2. The identification card of claim 1 wherein the verification message includes at least excerpts from the stored reference data.

3. The identification card of claim 2 wherein the verification message includes at least excerpts from the captured biometric data.

4. The identification card of claim 3 wherein the verification message is transmitted to a remote authentication system for additional verification.

5. The identification card of claim 4 wherein the remote authentication system includes remotely stored reference data that is different from the locally stored reference data.

6. The identification card of claim 4 wherein the on-board microprocessor uses a different matching algorithm than that used at the remote authentication system.

7. The identification card of claim 2 wherein the entire matching process is performed by the on-board processor and none of the captured biometric data is transmitted to the network.

8. The identification card of claim 2 wherein both the originally captured biometric data and any other "private" information stored in the on-board memory are not made available to any external processes.

9. The identification card of claim 2 wherein the card is ISO SmartCard compatible.

10. The identification card of claim 9 further comprising an ISO SmartCard processor.

11. The identification card of claim 10 wherein the security processor used for storing and processing the protected biometric data is functionally separated from the ISO SmartCard processor by a firewall.

12. The identification card of claim 10 wherein all external data to and from the security processor passes through the ISO SmartCard processor.

13. The identification card of claim 10 wherein all external data to and from the ISO SmartCard processor passes through the security processor.

14. The identification card of claim 10 wherein the security processor has a first connection used for loading data during a loading process and a second connection connected to an external network.

15. The identification card of claim wherein the first connection is permanently disabled after the loading process has been completed.

16. The identification card of claim 10 wherein the security processor used for storing and processing the protected biometric data is functionally separated from the ISO SmartCard processor by a firewall.

17. The identification card of claim 10 wherein:
the card comprises an upper magnetic stripe region and a lower embossed region;
the biometric sensor is a fingerprint sensor; and
the security processor, the ISO SmartCard processor and the fingerprint sensor are all located in a middle region between the upper region and the lower region.

18. The identification card of claim 2 wherein the biometric data includes fingerprint data and the sensor is a fingerprint sensor which captures data from a user's finger placed on the sensor.

19. The identification card of claim 18 wherein real-time feedback is provided while the user is manipulating his finger over the fingerprint sensor, thereby facilitating an optimal placement of the finger over the sensor.

20. The identification card of claim 18 wherein the matching process utilizes a hybrid matching algorithm that takes into account both minutiae and overall spatial relationships in the captured biometric data.

21. The identification card of claim 18 wherein the fingerprint sensor comprises a sheet of crystalline silicon supported by a backing plate.

22. The identification card of claim 21 wherein the backing plate comprises a glass epoxy layer sandwiched between two metal layers.

23. The identification card of claim 18 wherein the backing plate is reinforced by a carrier frame surrounding the sheet of silicon.

24. The identification card of claim 1 wherein the card further comprises means for restricting use of the card to a predetermined location. at least some of the captured

25. The identification card of claim 1 wherein at least some of the captured biometric data and the reference data are transmitted to a separate authentication server for secure verification of a user's identity priori to any grant of on-line access to an application server for processing of secure financial transactions involving that user.

26. The identification card of claim 25 wherein in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed in which a challenge character sequence is sent from the authentication sever to the identification card as, the identification card then uses the challenge character sequence and the match request to generate a challenge response which it then forwards to the application server, the application server then forwards the challenge response to the authentication server, which then verifies whether the challenge response is valid.

27. The identification card of claim 1 wherein the output from the card is used to obtain physical access into a secure area.

28. The identification card of claim 27 wherein a record of successful and unsuccessful access attempts is maintained on the card.